Trustwave®

# Supply Chain Security

## DIFFERENT, BUT THE SAME

**"The prototypical supply chain no longer exists. The vast network of suppliers, vendors, contractors, and remote staff with which businesses now interact is closer to an ecosystem."**

Nick Ellsmore
SVP, Consulting & Professional Services at Trustwave

Supply chain attacks have existed for decades. Yet it's only recently that the supply chain has become top of mind, with incidents like SolarWinds and Colonial Pipeline symptoms of an evolving landscape:

### The Rise of the digital economy

58% of all customer interactions and 55% of products/services are now digital.

### Distributed work

Prior to the pandemic, fewer than 6% of Americans worked from home —by September 2021, this increased to 45%.

### Increased outsourcing and offshoring

The global market for outsourcing hit $92.5 billion USD in 2019. The pandemic greatly amplified this.

## An Ecosystem Fraught with Risk

**"Why would someone try to crack a firewall when they can gain access through a hardware vulnerability or by targeting a contractor?"**

Nick Ellsmore
SVP, Consulting & Professional Services at Trustwave

Your supply chain is more than just vendors and business partners, but every entity with which you interact, even takeout restaurants. Given the variance in risk exposure, one must understand the different categories of risk:

### Geopolitical.

Nation-state threat actors and collateral damage from state-sponsored attacks. Disruptions from events such as COVID-19 may also qualify.

### Technology Compromise.

Compromised source code, unpatched vulnerabilities, and unsafe hardware. For example, Lapsus$ recently released a large quantity of Samsung's source code.

### Supplier Breach.

A supplier that suffers a cyberattack could either experience reduced service delivery or directly compromise your assets.

# How to Build a Better Supply Chain

**"A more secure and resilient supply chain starts with two core principles —due diligence and zero trust."**

Nick Ellsmore
SVP, Consulting & Professional Services at Trustwave

## Know who your suppliers are.

This includes the data they hold, their access permissions, and their criticality to your business operations.

## Supply chain resilience is multifaceted,and your assessments must be too.

You need to assess your suppliers and vendors from every angle, particularly their security maturity and supply chain risk management practices.

## Bring your suppliers into yoursecurity program.

This includes cybersecurity awareness, training, and participation in red team targeting events.

## Understand that suppliers aren't the enemy — and that you're a supplier, too.

Supply chain security needs to be collaborative. There is nothing to gain from an adversarial approach.

## Ensure you have the proper systems and tools in place.

This includes comprehensive endpoint detection and response capabilities, the capacity to ingest threat intelligence from suppliers, and streamlined, centralized management of your ecosystem.

## Don't be afraid to ask for help.

You'll never be able to achieve 100% supply chain visibility, especially when you're contending with a skills shortage. In this regard, the right partner can make a considerable difference, providing you with the resources, expertise, and guidance for a safer, stabler supply chain.

Trustwave®

www.trustwave.com